

Profesores

- Enrique Fernández Blanco
 - enrique.fernandez@udc.es
 - Teoría + Laboratorio
- Lara Pallas Quintela
 - O <u>lara.pquintela@udc.es</u>
 - Laboratorio
- Nieves Pedreira Souto
 - o nieves.pedreira@udc.es
 - Laboratorio
- Marco Antonio González Álvarez
 - o marco.antonio.agonzalez@udc.es
 - Laboratorio
- Martiño Rivera Dourado
 - o martino.rivera.dourado@udc.es
 - Laboratorio



Bibliografía

Referencias principales:

- Ariganello Ernesto. (2014) Redes CISCO. Guía de estudio para la certificación CCNA Routing y Switching. RA-MA
- Lammle Todd (2013) CCNA Routing and Switching Study Guide:
 Exams 100-101, 200-201, and 200-120. Sybex

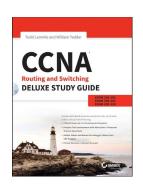
Material adicional:

- Stallings, W. (2004) Comunicaciones y Redes de Computadores.
 Pearson Prentice Hall.
- Meyers, M. (2009). Redes. Administración y mantenimiento (M. J. Pinilla Machado, Trans.): Anaya.
- Odom Wendell (2013) CCNET/CCNA ICND1 100-101 Official Cert Guide. Cisco Press.

Multimedia

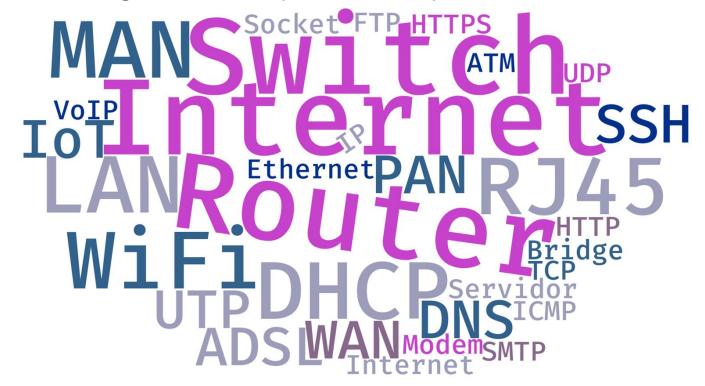
 Vídeo sobre el funcionamiento de las redes: Warriors of the Net (English): http://youtu.be/2kezQTo57yM





Calentamiento...

¿Cuáles de los siguientes conceptos no están presentes en una casa?



Objetivos Principales

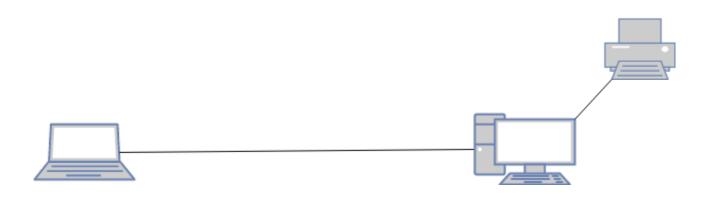
A final de curso, cualquier alumno debería de ser capaz de ...

- Entender qué es una red de ordenadores
- Ser capaz de clasificar una red por su extensión
- Identificar cuáles son y cómo funcionan los componentes más habituales de una red
- Ser capaz de definir y entender qué es un protocolo de red
- Comprender los protocolos de red más habituales
- Conocer el modelo OSI

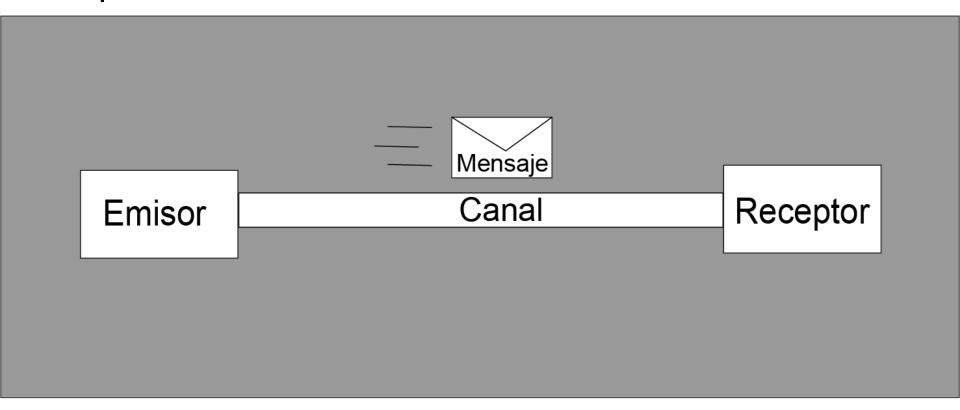
Conceptos Básicos

¿Que es una red de computadores?

Una **red informática** es un conjunto de dos o más ordenadores que están conectados por un medio físico a través de una tarjeta de red. Esa conexión puede ser mediante cable o inalámbrica y su objetivo es compartir recursos e información



Esquema de comunicación



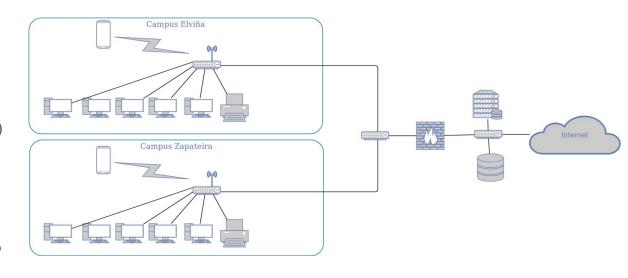
Componentes de una red

Las redes están compuestas por distintos dispositivos que colaboran entre ellos para compartir información entre el emisor y el receptor. Estos componentes se pueden clasificar en tres tipos:

- Dispositivos finales ("hosts")
 - Workstations, servidores, portátiles, PCs de sobremesas, tablets, smartphones,...
- Dispositivos de interconexión, intermedios o elementos activos
 - Eacilitan el envío de información entre el origen y destino
 - *Hubs*, *switches*, *routers*, *firewalls*, puntos de acceso...
- Elementos pasivos (Medios de transmisión)
 - Cable coaxial, fibra óptica, cable de par trenzado ...

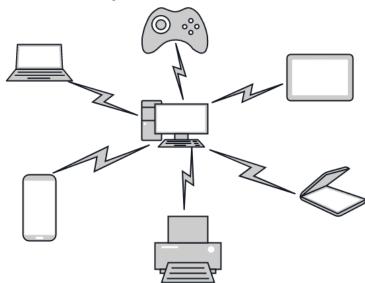
Clasificación por extensión

- Redes de Área Local (Local Area Network, LAN)
 - Cubren área relativamente pequeñas como una clase, un edificio, un campus
 - o Technologías: Ethernet, WiFi.
- Redes de Área Metropolitana
 (Metropolitan Area Network, MAN)
 - Están definidas sobre áreas similares a una metrópolis
 - Tecnologías: WiMax.
- Redes de Área Extensa (Wide Area Network, WAN)
 - Cubren areas muy amplias cómo pueden ser regiones, provincias, países o incluso el mundo
 - Tecnologías:
 - ADSL, cable módem, GPRS, UMTS, ... (Sólo de Acceso)
 - SDH, DWDM, ... (Entre proveedores)

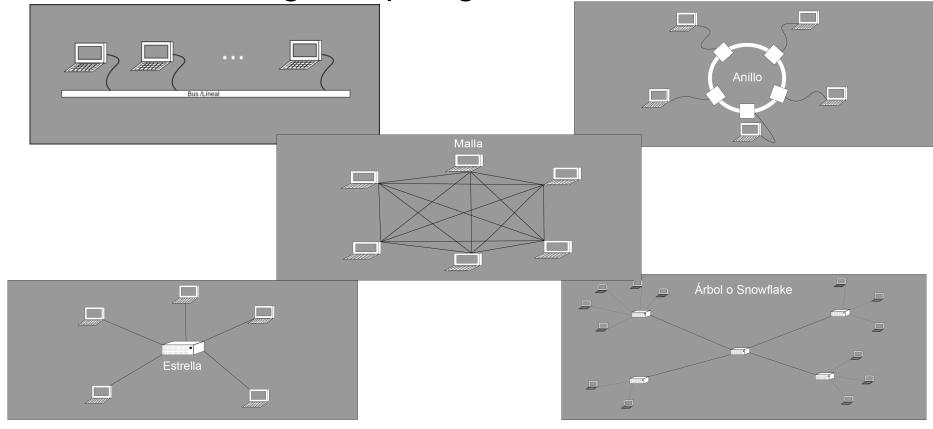


Clasificación por extensión

- Redes de Área Personal (Personal Area Network, PAN):
 - Definidas sobre área muy pequeñas. El objetivo principal es para comunicar dispositivos que se encuentran muy próximos entre ellos cómo, por ejemplo, un *smartphone*, impresoras, sensores,, etc.
 - Technologies: Bluetooth, infrarrojos.

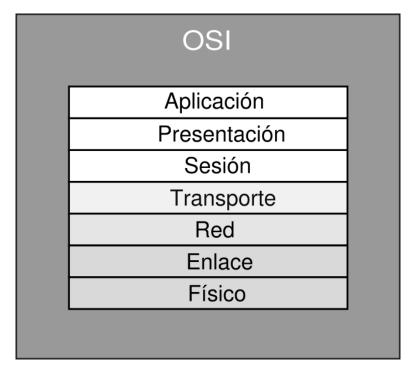


Clasificación segun topología



Un primer vistazo al modelo OSI

- Un modelo es simplemente una simplificación de un objeto real
- El modelo OSI es una versión simplificada de las capas de red de comunicaciones



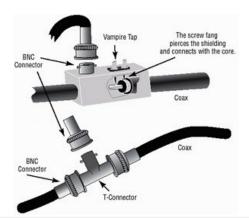
Modelo OSI

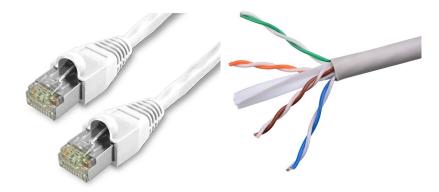


Medios de transmisión

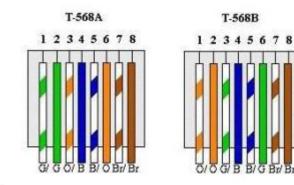


Cable Coaxial - RG58





Cable de cobre de par trenzado - RJ45

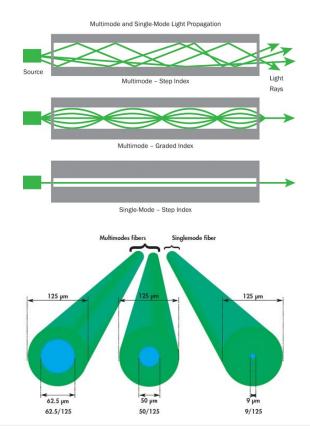


Medios de transmisión

Fibra Óptica



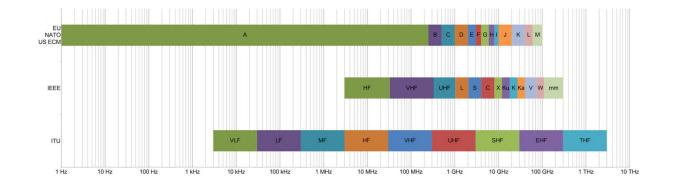




Medios de transmisión

Espectro radioeléctrico

- Infrarrojo
- Microondas
- Onda corta
- Onda media
- Onda Larga



Tarjeta de red (Network Interface Card, NIC)

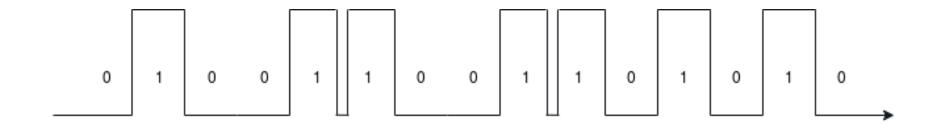
- Está directamente conectada al ordenador y proporciona un punto de conexión a la red
- Facilita la conexión física al medio de transmisión que puede ser cableado o inalámbrico
- Es el dispositivo responsable de crear y recibir la información en forma de señales adecuadas para llegar al siguiente dispositivo





Tarjeta de red (Network Interface Card, NIC)

 Las NICs envían y reciben datos binarios mediante impulsos eléctricos, pulsos luminosos u ondas de radio

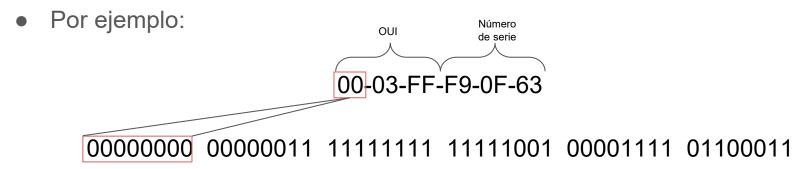


Modelo OSI



Dirección MAC

- Cada NIC tiene un identificador único que se conoce cómo Dirección MAC Address (*Media Access Control*)
- Las direcciones MAC son identificadores compuestos por <u>48 bits</u> que se escriben en notación hexadecimal



Hex	0	1	2	3	4	5	6	7	8	9	А	В	С	D	E	F
Bin	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111

¿Cómo se transmiten los datos?

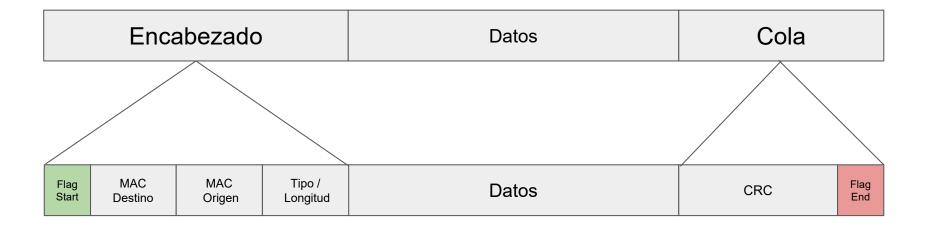
Datagrama de nivel de enlace

Encabezado	Datos	Cola
------------	-------	------

CRC: Cyclic Redundancy Check

¿Cómo se transmiten los datos?

Datagrama de nivel de enlace



CRC: Cyclic Redundancy Check

Tecnologías de Red: Ethernet

- ¿Cómo es posible que los dispositivos de una red se entiendan entre ellos?
 - Ethernet Standard (IEEE 802.3)
 - Garantiza la compatibilidad de los dispositivos en una red
 - Las tarjetas de red Ethernet utilizan un método de control de acceso al medio conocido cómo:

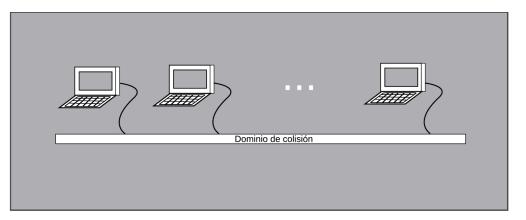
CSMA/CD (Carrier Sense Multiple Access / Collision Detect)

- Cada dispositivo en la red respecta estrictamente su turno para hablar, de tal manera que si un dispositivo quiere transmitir debe escuchar el medio hasta que ningún otro esté transmitiendo
- Sin embargo ... a veces ocurren colisiones aun siendo muy cuidadosos y es necesario el detectarlas
- Existen dos tipos:
 - Legacy Ethernet
 - Ethernet conmutado



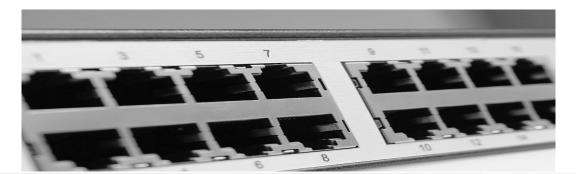
Informática Básica Curso 2022/23

- La implementación más antigua de Ethernet centrada en resolver los problemas causados por el cable coaxial
- Una de las estaciones pone una trama en el cable y todas las demás reciben el mismo mensaje
- Cada estación se queda sólo con las tramas que la tienen a ella misma como destinataria.



Dominio de Colisión: Es el conjunto de dispositivos que comparten un medio físico para transmitir y, por tanto, compiten por él

- Dispositivos intermedios
 - Repetidor de red
 - Permite superar las restricciones físicas establecidas por la atenuación de la señal en el medio
 - Hub o repetidor multipuerto
 - Repite y concentra las señales de tráfico de una red
 - Recibe datos por un puerto y lo reenvía y regenera en el resto de puertos



Informática Básica Curso 2022/23

- Problemas sin resolver
 - Ni los repetidores ni los hubs procesan los datos. Sólo regeneran y sincronizan la señal
 - Ancho de banda compartido
 - Colisiones

- Problemas sin resolver
 - Ni los repetidores ni los hubs procesan los datos. Sólo regeneran y sincronizan la señal
 - Ancho de banda compartido
 - Colisiones

Solución:

- Creación de múltiples dominios de colisión
- Dispositivos de red más avanzados
 - Bridges y Switches

Tecnología Ethernet Conmutada

- Un puente o bridge es un dispositivo que interconecta redes y toma decisiones acerca del reenvío de las tramas. Para ello, utiliza las direcciones MAC como fuente de información
- Los Bridges mantienen una tabla de direcciones que asocia una MAC de destino con el puerto físico donde se encuentra (Content-Addressable Memory Table, CAM Table)
- Este proceso permite al bridge redirigir los datos sólo al puerto físico donde encontrará al destinatario (esta es la principal diferencia con el HUB)
 - Se crean por tanto múltiples dominios de colisión (1 por cada puerto)

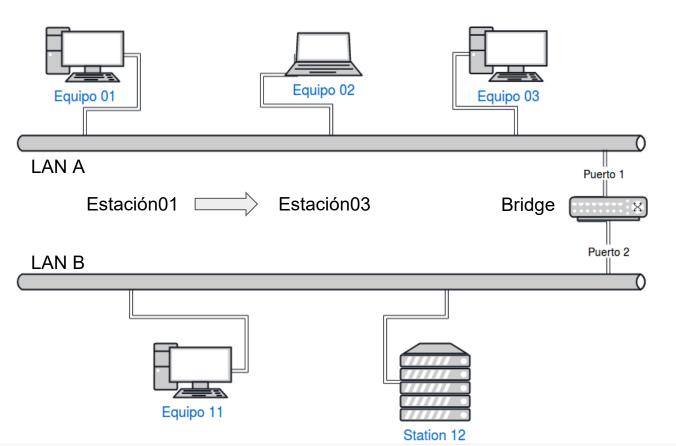


Tabla del Bridge					
Estación01	Puerto 1				
Estación02	Puerto 1				
Estación03	Puerto 1				
Estación11	Puerto 2				
Estación12	Puerto 2				

Informática Básica Curso 2022/23

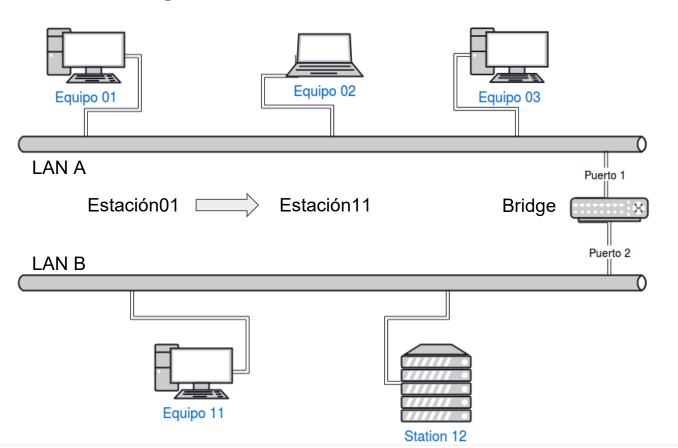


Tabla del Bridge					
Estación01	Puerto 1				
Estación02	Puerto 1				
Estación03	Puerto 1				
Estación11	Puerto 2				
Estación12	Puerto 2				

Informática Básica Curso 2022/23

¿Cómo funciona?

- 1. Actualizar la tabla de direcciones MAC
- Cuando se recibe una trama en un puerto físico del bridge, se crea una nueva entrada en la tabla. Esa nueva entrada asocia MAC del origen con el número de puerto por el que se recibió
- Así, el bridge sabrá el puerto en el que está ubicado si recibe una trama con destino ese disposi
- El bridge elimina de la tabla una MAC si no está activa durante un periodo limitado de tiempo (habitualmente en torno a 300 segundos)

¿Cómo funciona?

- 2. Envío de tramas: Buscar la MAC destino en la tabla
- Está en la lista, entonces la trama se envía sólo por el puerto que tiene asociado
- No está en la lista (el dispositivo no envió nada de tráfico previamente o su entrada en la tabla ha caducado): la trama se reenvía por todos los puertos, excepto por el que se recibió.
 - Todos los dispositivos reciben la trama pero sólo la que tenga la MAC de destino responderá. Entonces el bridge podrá registrar el dispositivo como una nueva entrada de la tabla CAM
 - Mientras que la entrada permanezca en la tabla, el bridge no volverá a inundar (flood) todos

los puertos por tramas dirigidas a esa dirección MAC
UNIVERSIDADE DA CORUÑA
Informática Básica

- Muchas de las tecnologías de acceso múltiple, como, por ejemplo, Ethernet, tienen algunos paquetes/tramas especiales denominados de difusión o broadcast
 - Uno de las características más importantes de estos paquetes es que tienen dirección de destino MAC FF-FF-FF-FF
 - Estos paquetes son recibidos y procesados por todos los dispositivos en una red
 - Este tráfico es necesario para administrar la red y su flujo, por lo tanto no puede ser eliminado.
 - El número de dispositivos en una red es proporcional a la cantidad de tráfico broadcast en la misma. Más dispositivos implican más tráfico de broadcast que afecta al rendimiento de la red en general y de los dispositivos en particular
- Conclusión: Es necesario mantener el tamaño de los dominios de broadcast tan pequeño como se pueda

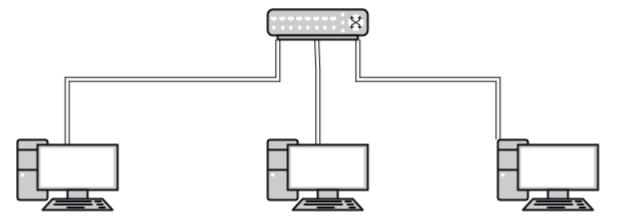
- Problemas generados por el uso de bridges:
 - Incremento de la latencia. Los bridges son habitualmente dispositivos lentos que tienen un retardo en el procesado de las tramas
 - Procesado mediante software: sistema operativo, acceso a memoria, etc.
 - No permiten concentrar grandes cantidades de dispositivos. Esto se debe a que el número de puertos de este tipo de dispositivos es muy limitado (2, 4, 8...)

Solución: Switches o Conmutadores

- Un conmutador o switch es un dispositivo que interconecta redes de manera similar a como lo hace un bridge, pero es más rápido
 - Tabla CAM (Content-Addressable Memory)

- Principal diferencia: los switches realizan sus funciones mediante hardware mientras que los bridges las realizan mediante software. Esas funciones incluyen el aprendizaje de direcciones, la selección de puertos y la conmutación de tramas
 - Los switches son los dispositivos más habituales en la capa de acceso de las redes corporativas
 - Habitualmente, los switches tienen una densidad mayor de puertos que los bridges (16, 32, 64, ...)

- El escenario más habitual en una LAN actualmente :
 - Hosts conectados a un switch
 - Un único host por puerto



Modelo OSI



Protocolo IP

- Las direcciones MAC tienen una estructura plana que no permite jerarquía.
- Este hecho tiene como problema que las direcciones MAC no son escalables
- Se necesita algo para unificar las tecnologías subyacentes (Ethernet, ADSL, PPP, ...)

Se necesita definir un protocolo en la capa de red

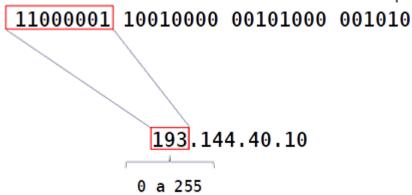
IP: Internet Protocol (IPv4)

Funcionamiento IP

- ¿Cómo envía datos un dispositivo a otra red?
 - 1. Necesita una manera en la que con la dirección IP identifique la LAN
 - Permitir la interconexión de LANs mediante el uso de routers y ofreciendo un sistema para usar las IPs para encaminar correctamente los paquetes
 - Dar a todos los hosts de una red un mecanismo para identificar si un paquete es para un dispositivo en la LAN o debe ser encaminado hacia otra red

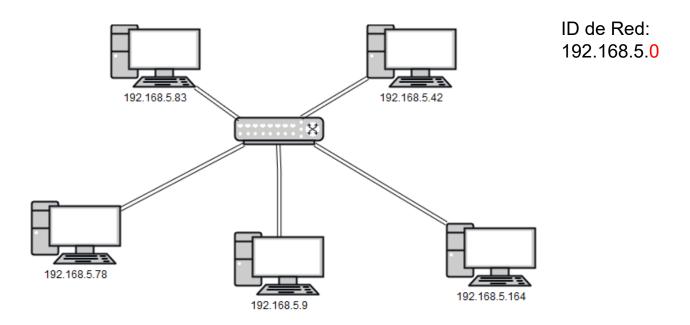
Direcciones IP

- Secuencias de 32 bits que identifican un dispositivo conectado a una red de forma no ambigua.
- Jerarquía en las direcciones:
- Formadas por dos partes
 - Un ID de la red lógica (Dominio de difusión)
 - Un ID del host dentro de la red lógica
- Habitualmente se escriben en formato decimal separado por punto



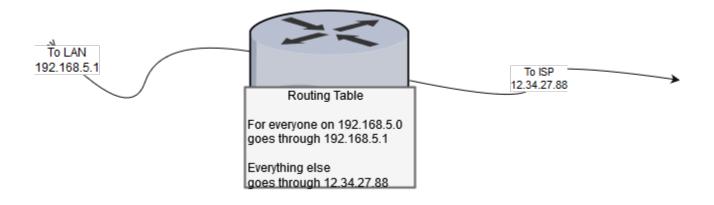
ID de Red en las direcciones IP

- Las direcciones IP están compuestas por dos partes: ID de red e ID de host.
 - o Todos los dispositivos de una red tienen el mismo ID de red
 - o Para diferenciar los hosts en una red lógica se utiliza el ID de host o dirección local



Interconexión

- Las LANs se organizan en redes más grandes, donde los routers son necesarios para administrar la comunicación entre ellas
- Los routers usan las direcciones IP para decidir el destino de un paquete.
- Los routers necesitan tener una IP asignada en cada red a la que están directamente conectados



Router

- El dispositivo responsable de conectar dos o más redes
- Funciones Principales:
 - Escoger un ruta para los paquetes (enrutamiento)
 - Transmitir los paquetes por el interfaz adecuado (conmutación)
- Sobre las IPs, los routers escogen la interfaz de salida o la ruta para cada paquete en función de la IP de destino.
 - Para conseguir este objetivo, los routers mantienen una tabla de enrutamiento en memoria, esta tabla contiene la información de todas las redes conocidas. Dicha tabla asocia ID de red con el interfaz donde se puede encontrar

Trabajando con IP

 ¿Cómo puede IP ayudarnos a identificar si un paquete es para un dispositivo de la red o de otra red?

¿Están 10.10.101.5 y 10.10.102.30 en la misma red?

¿Están 192.168.0.5 y 192.168.10.6 en la misma red?

Clases de direcciones IPv4

Clase	Bits más Significativos	Primer Octeto	Bits de red	Bits de Host	Host en la red
A	0	0-127	1+7	24	16.277.214
В	10	128-191	2+14	16	65.534
С	110	192-223	3+21	8	254
D	1110	224-239	Multicast		-
Е	1111	240-255	Experimental		-

Clases de direcciones IPv4

¿Cuál es el identificador de red para las siguientes direcciones IP?

- 10.10.100.5
- 130.100.1.4
- 193.144.48.30
- 255.100.200.8

Direcciones IPv4

Problemas:

- Una organización que necesita 2.000 direcciones, tendría que adquirir una licencia B, con lo que se malgastarían 63.000 direcciones, o sería mejor que contratase 8 licencias C
- Las direcciones IP se agotaron en nada
- Enrutamiento de Interdominios sin Clases (CIDR, Classless InterDomain Routing)

Solución:

Se necesita modificar el direccionamiento IP (RFC 950, Internet Standard Subnetting Proc)

Direccionamiento IPv4

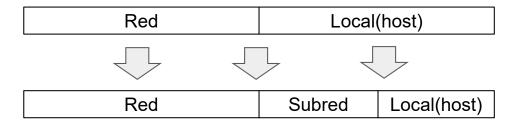
- Se introduce un tercer nivel en el espacio de direcciones IP. Los tres niveles de direccionamiento son:
 - Dirección de red: Es un campo de longitud fija que identifica a la propia red en Internet. La longitud de este campo depende de la clase de la dirección.
 - Dirección de subred: Es un campo de longitud variable que permite utilizar cualquier número de bits de la parte host para codificar la subred (restricciones)
 - o Dirección local o de "host": Identifica al dispositivo dentro de la subred local

 Para indicar cuántos bits forman el campo de subred y cuántos forman el campo de host fue necesario introducir un elemento adicional en el direccionamiento: máscara de subred

- Una máscara de subred es una cadena de 32 bits.
- Una serie de "unos" seguida de una serie de "ceros".
- Se representa en formato decimal punteado. Ejemplos:

255.255.255.0 255.255.255.128 255.0.0.0

Se usa para diferenciar la dirección de red de la dirección de host.



Classes of IPv4 Addresses

Clase	Bits más significativos	Primer Octeto	Bits de red	Bits de host	Host en la red	Máscara de Red
А	0	0-127	1+7	24	16.277.214	255.0.0.0
В	10	128-191	2+14	16	65.534	255.255.0.0
С	110	192-223	3+21	8	254	255.255.255.0
D	1110	224-239	Multicast		-	-
Е	1111	240-255	Experir	mental	-	-

Cuando se alinea una IP con su máscara de subred correspondiente en binario, la parte de la dirección IP que coincide con la máscara de subred es el ID de red. La parte que coincide con los ceros es el ID del host

	Decimal	Binario
IP	193.17.17.205	11000001.00010001.00010001.11001101
Máscara	255.255.255.0	11111111.11111111.11111111 00000000
ID de red	193.17.17.0	11000001.00010001.00010001 00000000
ID de Host	x.x.x.205	11001101

Cuando se alinea una IP con su máscara de subred correspondiente en binario, la parte de la dirección IP que coincide con la máscara de subred es el ID de red. La parte que coincide con los ceros es el ID del host

	Decimal	Binario
IP	193.17.17.205	11000001.00010001.00010001.11001101
Máscara	255.255.255.192	11111111.11111111111111111111111111111
ID de red	193.17.17.192	11000001.00010001.00010001.11000000
ID de host	x.x.x.13	001101

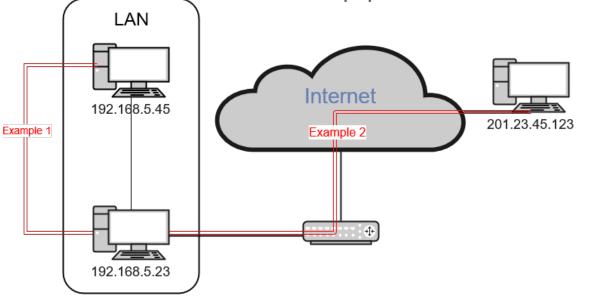
Otra representación para las máscaras de subred:

	Decimal	Binario
IP	192.168.5.23	11000000.10101000.00000101.00010111
Másc.	255.255.255.0	11111111111111111111111100000000



¿Cómo funciona IP con la máscara?

- Veremos dos ejemplos:
- Ejemplo 1: Comunicación entre dos equipos de la misma red.
- Ejemplo 2: Comunicación entre dos equipos en diferentes redes.



¿Cómo funciona IP con la máscara?

- Ejemplo 1. A (192.168.5.23) quiere enviar un paquete a B (192.168.5.45)
 - ¿Están en la misma LAN?

	Decimal	Binario
IP A	192.168.5.23	11000000.10101000.00000101.00010111
Másc.	255.255.255.0	111111111111111111111111100000000
IP B	192.168.5.45	11000000.10101000.00000101.00101100

SÍ: hay que averiguar la MAC de B (con ARP) y puede enviarse el paquete.

¿Cómo funciona IP con la máscara?

- Ejemplo 2: A (192.168.5.23) quiere enviar un paquete a C (201.23.45.123)
 - ¿Están en la misma LAN?

	Decimal	Binary
IP A	192.168.5.23	11000000.10101000.00000101.00010111
Másc.	255.255.255.0	11111111111111111111111100000000
IP C	201.23.45.123	10110110.11011101.00000011.00110111

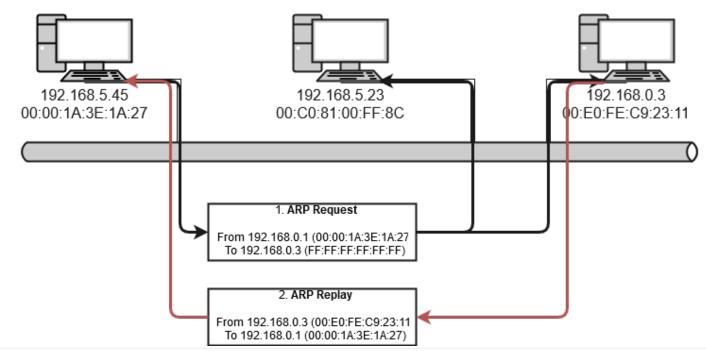
NO: los dispositivos no están en la misma red. El paquete debe enviarse por la puerta de enlace predeterminada

De la puerta de enlace se conoce la IP -> hay que obtener la MAC (con ARP)

ARP (Address Resolution Protocol)

El protocolo de resolución de direcciones (ARP) es la forma en que las redes TCP/IP "averiguan" las direcciones MAC basándose en las direcciones IP de

destino



ARP (Address Resolution Protocol)

- Averiguar la MAC de un equipo implica realizar una consulta que llega a todos los equipos de la LAN
 - Consume tiempo
 - Genera tráfico
- Para evitar preguntar constantemente la MAC de un equipo, cada equipo guarda en memoria aquellas IP que va "resolviendo". Es decir, cada vez que averigua la MAC de un equipo, almacena el par (IP, MAC), para evitar tener que preguntarla de nuevo
- Esta memoria se llama caché ARP.
 - Los SOs proporcionan comandos para consultarla (ver práctica)

Direcciones IP estáticas y dinámicas

Estáticas

- o Implican configurar en cada dispositivo toda la información necesaria
 - Dirección IP
 - Máscara de red
 - Puerta de enlace (Default Gateway)
 - DNS
- Los cambios en la red pueden ser fuente de numerosos problemas

Dinámicas

- Se asignan mediante un servidor DHCP (Protocolo de Configuración Dinámica de Host o Dynamic Host Configuration Protocol)
- O Cada uno de los clientes se configuran mediante el uso del protocolo DHCP.

DHCP (Dynamic Host Configuration Protocol)

- ¿Cómo funciona?
 - Necesita un servidor de DHCP en la LAN
 - Cliente pregunta: ¿algún servidor DHCP por ahí?
 - El servidor DHCP devuelve:
 - Una IP que esté libre (del rango configurado)
 - Máscara de red
 - Puerta de enlace
 - DNS
 - El cliente acepta la configuración
 - O El servidor envía el acuse de recibo (ACK)

Direcciones IP especiales

- Direcciones de enlace local:
 - o Rango:
 - **1**69.254.0.0/16
 - Permiten la comunicación con otros dispositivos que están en el mismo dominio de broadcast, única y exclusivamente
 - Se usan cuando no se le ha asignado una IP a una interfaz ni manualmente, ni por medio de un servidor DHCP.

Direcciones APIPA (Entornos Microsoft)

Direcciones IP especiales

- Direcciones privadas:
 - Rango:
 - 10.0.0.0 a 10.255.255.255 (1 licencia clase A).
 - 172.16.0.0 a 172.31.255.255 (16 licencias clase B).
 - 192.168.0.0 a 192.168.255.255 (256 licencias clase C).
 - Los routers no las encaminan a través de la red pública
 - NO se pueden usar en Internet
 - Cualquiera puede usar direcciones IP privadas, pero no son útiles para sistemas que tengan que acceder a Internet, salvo que se use NAT (Network Address Translation)

Direcciones IP especiales

- Interfaz de loopback o de bucle de retorno:
 - Interfaz de red virtual (no está conectada a ningún otro dispositivo).
 - Suele tener asignada un IP de la red 127.0.0.0/8., rango usado para designar al propio dispositivo
 - La IP más comúnmente asignada es 127.0.0.1, también conocida como dirección de localhost
 - Es posible hacer ping a la interfaz de loopback para probar la configuración de TCP/IP en el host local

NAT (Network Address Translation)

 Mecanismo que permite que múltiples dispositivos con IP privada puedan acceder a Internet usando un conjunto reducido de direcciones IP públicas.

Necesario, debido al agotamiento de direcciones IPv4.

• Un router NAT cambia la dirección de origen privada (y, normalmente, el puerto) en cada paquete de salida. Estas traducciones se almacenan en una tabla, para saber a donde enviar los paquetes de respuesta.

IPv6

- Soluciona los siguientes problemas de IPv4:
 - Jerarquía Geográfica
 - Prioridad en el tráfico
 - Escasez de direcciones
 - Cabecera de longitud variable de la cabecera
- Cambio de direcciones de 32 bits a 128 bits (RFC 3587)
 - 24ae:0000:f2f3:0000:0000:0678:b3aa;6177/64
 - 24ae:0:f2f3:0:0:678:b3aa:6177/64
 - 24ae:0:f2f3::678;b3aa:6177/64
- Loopback ::1
- Tipos de tráfico: unicast, multicast y anycast, NO broadcast
- Más de 640 sextilliones de direcciones
- Direcciones Locales FE80::/10
 - Mapeo de IPv4 0::ffff:0:0/96
 - 10.0.0.1 -> 0::ffff:0:0:A00:1



Modelo OSI



Protocolos de transporte

- Un equipo puede enviar datos a otro, pero...
- ¿Cómo sabe el equipo receptor qué paquete tiene que pasar a cada aplicación (navegador, messenger, outlook, eMule, etc.)?
 - o Con la IP sólo no se puede
 - Se necesita el número de puerto

IP Origen + Puerto Origen / IP Destino + Puerto Destino Port = SOCKET 193.147.50.21:15535 / 193.144.48.60:80

- En Internet hay dos protocolos fundamentales en esta capa:
 - TCP (Orientado a Conexión)
 - UDP (No Orientado a Conexión)

Puertos

- Un puerto es un valor que permite identificar de forma única a cada uno de los procesos que emplean un mismo protocolo de transporte.
 - o Rango: 0 a 65.535
- Las aplicaciones "servidor" suelen tener puertos "fijos". Ejemplo:
 - o HTTP 80
 - HTTPS 443
 - FTP 21
 - o SSH 22
 - SMTP 25
- Las aplicaciones "cliente" se ejecutan en puertos "aleatorios
 - O Más info en: http://www.iana.org/assignments/port-numbers

Protocolos de capa de transporte. TCP

- TCP (Transmission Control Protocol o Protocolo de Control de Transmisión) es un protocolo en el cual:
 - Dos equipos que quieren comunicarse, primero se saludan, a continuación intercambian información y finalmente se despiden
 - El receptor confirma que ha recibido la información con un OK o bien solicita que se le envíe de nuevo
 - Es algo parecido a una conversación telefónica
 - Se dice que es "orientado a conexión" y "fiable"
 - Ejemplos de aplicaciones que utilizan TCP: navegador, lector de correo...

Transport protocols: UDP

- UDP (User Datagram Protocol o Protocolo de Datagrama de Usuario) es un protocolo en el cual
 - Un equipo envía un mensaje a otro y no se queda esperando respuesta (simplemente confía en que lo reciba o sencillamente no le importa)
 - Es algo parecido a enviar una postal
 - Se dice que es "no orientado a conexión" y "no fiable"
 - La base de QUIC futura base de la web en sustitución de TCP
 - Quick UDP Internet Connections

■ Ejemplos de aplicaciones que utilizan UDP: DNS, algunos juegos on-line, VoIP. ...

Nombres de dominio y DNS

- Los humanos manejamos nombres de dominio (e.g. www.google.com)
 no direcciones IP
- Cada nombre de dominio está relacionado con una IP:

www.google.es	72.14.235.104
www.facebook.com	66.220.153.19
zipi.udc.es	193.144.48.30
zape.udc.es	193.147.40.100

• Existen máquinas denominadas Servidor de Nombres de Dominio o DNS (de sus siglas en inglés Domain Name Server), que se encargan de realizar esta

UNIVERSIDADE DA CORUÑA

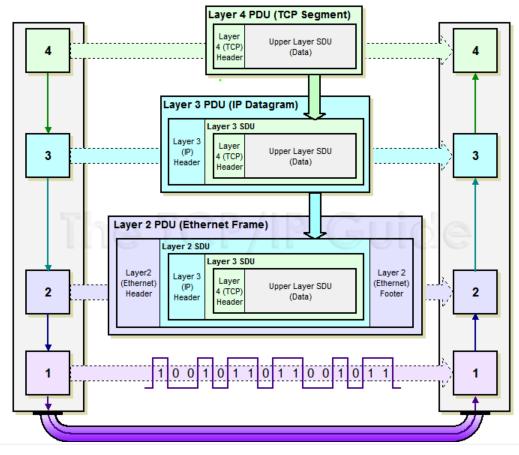
Nombres de dominio y DNS

- Un DNS recibe preguntas del tipo "Quién es www.google.com?" y responde cosas como "72.14.235.104"
- Cada organización suele disponer de sus propios DNS:
 - DNS UDC: zipi.udc.es
- También hay organizaciones que ofrecen DNS públicos:
 - Google (IPv4):
 - **8.8.8.8**
 - 8.8.4.4
 - OpenDNS (IPv4):
 - **2**08.67.222.222
 - 208.67.220.220
 - Cloudflares
 - 1.1.1.1
 - **1.0.0.1**
 - Norton

Modelo OSI

Num	Capa	Unidad de intercambio	Descripción
7	Aplicación	APDU	Provee de servicios generales (navegador, Cliente de correo, eMule, etc.)
6	Presentación	PPDU	Formateo de datos cómo compresión, cifrado, etc.
5	Sesión	SPDU	Administración de la sesión
4	Transporte	TPDU	Habilita el transporte punto a punto
3	Red	paquete	Enruta las unidades de información
2	Enlace	datagrama	Habilita la comunicación entre dispositivos que comparten el medio físico
1	Físico	bit	Transmite un bit a través de un medio físico

Transmisión Real vs Transmisión Teórica



Modelo TCP/IP vs. Modelo OSI

TCP/IP	OSI
	Aplicación
Aplicación	Presentación
_	Sesión
Transporte	Transporte
Red	Red
Interface de Red	Enlace
interrace de Ned	Físico